Practitioner's Docket No. NAI1P020/01.139.01 *PATENT*

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of: Chris A. Barton et al.

Application No.: 09/916,600 Group No.: 2137
Filed: 07/26/2001 Examiner: Pyzocha, Michael J.
For: SYSTEM, METHOD AND COMPUTER PROGRAM PRODUCT FOR ANTI-VIRUS SCANNING IN A STORAGE SUBSYSTEM

Mail Stop Appeal Briefs – Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

TRANSMITTAL OF APPEAL BRIEF
(PATENT APPLICATION--37 C.F.R. § 41.37)

1. This brief is in furtherance of the Notice of Appeal filed June 2, 2005, a substitute for the Appeal Brief filed October 13, 2005, and in response to the Notification of Non-Compliant Appeal Brief mailed on September 21, 2007.

2. STATUS OF APPLICANT

   This application is on behalf of other than a small entity.

3. FEE FOR FILING APPEAL BRIEF

   Pursuant to 37 C.F.R. § 41.20(b)(2), the fee for filing the Appeal Brief is:

other than a small entity	$510.00
Appeal Brief fee due	**$510.00**

4. EXTENSION OF TERM

   The proceedings herein are for a patent application and the provisions of 37 C.F.R. § 1.136 apply.

   Applicant believes that no extension of term is required. However, this conditional petition is being made to provide for the possibility that applicant has inadvertently overlooked the need for a petition and fee for extension of time.

5. TOTAL FEE DUE

The total fee due is:

Appeal brief fee	$0.00 (previously paid on July 7, 2005)
Extension fee (if any)	$0.00
TOTAL FEE DUE	**$0.00**

6. FEE PAYMENT

Applicant believes that no fees are due in connection with the filing of this paper because the appeal brief fee was paid with a previous submission. However, the Commissioner is authorized to charge any additional fees that may be due (e.g. for any reason including, but not limited to, fee changes, etc.) to Deposit Account No. 50-1351 (Order No. NAI1P020).

7. FEE DEFICIENCY

If any additional extension and/or fee is required, and if any additional fee for claims is required, charge Deposit Account No. 50-1351 (Order No. NAI1P020).

Date: October 22, 2007

/KEVINZILKA/
Signature of Practitioner

Reg. No.: 41,429
Tel. No.: 408-971-2573
Customer No.: 28875

Kevin J. Zilka
Zilka-Kotab, PC
P.O. Box 721120
San Jose, CA 95172-1120

PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of:	
Barton et al.	Group Art Unit: 2137
Application No. 09/916,600	Examiner: Pyzocha, Michael J.
Filed: 07/26/2001	Atty. Docket No. NAI1P020/01.139.01
For: SYSTEM, METHOD AND COMPUTER PROGRAM PRODUCT FOR ANTI-VIRUS SCANNING IN A STORAGE SUBSYSTEM	Date: 10/22/2007

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

ATTENTION: Board of Patent Appeals and Interferences

SUBSTITUTE APPEAL BRIEF (37 C.F.R. § 41.37)

This brief is in furtherance of the Notice of Appeal filed June 2, 2005, a substitute for the Appeal Brief filed October 13, 2005, and in response to the Notification of Non-Compliant Appeal Brief mailed on September 21, 2007 (see attached). While appellant disagrees with the Examiner as to whether the alleged deficiencies exist in the original Appeal Brief, a Substitute Appeal Brief with appropriate edits is nevertheless submitted to expedite prosecution.

The fees required under § 1.17, and any required petition for extension of time for filing this brief and fees therefor, are dealt with in the accompanying TRANSMITTAL OF APPEAL BRIEF.

This brief contains these items under the following headings, and in the order set forth below (37 C.F.R. § 41.37(c)(i)):

I REAL PARTY IN INTEREST

II RELATED APPEALS AND INTERFERENCES

III STATUS OF CLAIMS

IV STATUS OF AMENDMENTS

V SUMMARY OF CLAIMED SUBJECT MATTER

VI GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

VII ARGUMENT

VIII CLAIMS APPENDIX

IX EVIDENCE APPENDIX

X RELATED PROCEEDING APPENDIX

The final page of this brief bears the practitioner's signature.

I REAL PARTY IN INTEREST (37 C.F.R. § 41.37(c)(1)(i))

The real party in interest in this appeal is McAfee, Inc.

II RELATED APPEALS AND INTERFERENCES (37 C.F.R. § 41.37(c) (1)(ii))

With respect to other prior or pending appeals, interferences, or related judicial proceedings that will directly affect, or be directly affected by, or have a bearing on the Board's decision in the pending appeal, there are no other such appeals, interferences, or related judicial proceedings.

A Related Proceedings Appendix is appended hereto.

III STATUS OF CLAIMS (37 C.F.R. § 41.37(c) (1)(iii))

A. TOTAL NUMBER OF CLAIMS IN APPLICATION

Claims in the application are: 1-2, 4-7, 10-12, 14-18, 20-23 and 26-43

B. STATUS OF ALL THE CLAIMS IN APPLICATION

1. Claims withdrawn from consideration: None
2. Claims pending: 1-2, 4-7, 10-13, 14-18, 20-23 and 26-43
3. Claims allowed: None
4. Claims rejected: 1-2, 4-7, 10-13, 14-18, 20-23 and 26-43
5. Claims cancelled: 3, 8-9, 19, and 24-25

C. CLAIMS ON APPEAL

The claims on appeal are: 1-2, 4-7, 10-13, 14-18, 20-23 and 26-43

See additional status information in the Appendix of Claims.

IV STATUS OF AMENDMENTS (37 C.F.R. § 41.37(c)(1)(iv))

As to the status of any amendment filed subsequent to final rejection, an amendment was filed on 04/28/2005 after a final rejection mailed 03/22/2005, which was not entered by the Examiner.

V SUMMARY OF CLAIMED SUBJECT MATTER (37 C.F.R. § 41.37(c)(1)(v))

With respect to a summary of Claim 1, as shown in Figures 2 and 4, a method for scanning data read from storage is provided including receiving a request for data saved in storage from a central processing unit (e.g. item 402 of Figure 4). In use, the requested data is scanned for malicious code (e.g. item 406 of Figure 4) and the data is transmitted from the storage to the central processing unit if malicious code is not found in the data during the scanning (e.g. item 410 of Figure 4). In addition, the scanning is performed by a scanning module coupled to a storage subsystem controller (e.g. items 208 and 204 of Figure 2). Furthermore, a user is allowed to disable the scanning module, and data is precluded from being transmitted from the storage to the central processing unit upon the disabling of the scanning module (e.g. items 404, 418 and 416 of Figure 4). Note page 6, and page 9, line 6 – page 10, line 31, for example.

With respect to a summary of Claim 17, as shown in Figures 2 and 4, a computer program product for scanning data read from storage is provided. Computer code is included for receiving a request for data saved in storage from a central processing unit (e.g. item 402 of Figure 4). In addition computer code is included for scanning the requested data for malicious code (e.g. item 406 of Figure 4). Computer code is also included for transmitting the data from the storage to the central processing unit if malicious code is not found in the data during the scanning (e.g. item 410 of Figure 4). Further, the scanning is performed by a scanning module coupled to a storage subsystem controller (e.g. items 208 and 204 of Figure 2). Also, a user is allowed to disable the scanning module, and data is precluded from being transmitted from the storage to the central processing unit upon the disabling of the scanning module (e.g. items 404, 418 and 416 of Figure 4). Note page 6, and page 9, line 6 – page 10, line 31, for example.

With respect to a summary of Claim 33, as shown in Figures 2 and 4, a method for scanning data written to storage is provided including receiving a request for data to be written in storage, the request being received from a central processing unit (e.g. item 402 of Figure 4). Further, the data is scanned for malicious code (e.g. item 406 of Figure 4). In addition, the data is written to the storage if malicious code is not found in the data during the scanning (e.g. item 410 of Figure 4). The scanning is performed by a scanning module coupled to a storage subsystem controller

(e.g. items 208 and 204 of Figure 2). Also, a user is allowed to disable the scanning module, and data is precluded from being transmitted to the storage from the central processing unit upon the disabling of the scanning module (e.g. items 404, 418 and 416 of Figure 4). Note page 6, and page 9, line 6 – page 10, line 31, for example.

With respect to a summary of Claim 34, as shown in Figures 2 and 4, a computer program product is provided for scanning data written to storage. Computer code is included for receiving a request for data to be written in storage, the request being received from a central processing unit (e.g. item 402 of Figure 4). Computer code is also included for scanning the data for malicious code (e.g. item 406 of Figure 4). Still yet, computer code is included for writing the data to the storage if malicious code is not found in the data during the scanning (e.g. item 410 of Figure 4). Further, the scanning is performed by a scanning module coupled to a storage subsystem controller (e.g. items 208 and 204 of Figure 2). Also, a user is allowed to disable the scanning module, and data is precluded from being transmitted to the storage from the central processing unit upon the disabling of the scanning module (e.g. items 404, 418 and 416 of Figure 4). Note page 6, and page 9, line 6 – page 10, line 31, for example.

With respect to a summary of Claim 35, the above summary of Claim 1 is incorporated, at least in part, by reference. Further provided is a system that includes storage (e.g. item 202 of Figure 2) for saving data therein, a storage subsystem controller (e.g. 204 of Figure 2) coupled to the storage for controlling access to the data saved therein, and a central processing unit (e.g. item 206 of Figure 2) coupled to the storage subsystem controller for issuing read requests for reading the data saved therein for processing purposes, and write requests for writing data to the storage. Also included is a scanning module (e.g. item 208 of Figure 2) coupled to the central processing unit and the storage subsystem controller. The scanning module is adapted for identifying the requests from the central processing unit, and scanning the data for malicious code in response to the requests. An event manager module (e.g. item 346 of Figure 3) is coupled to the scanning module and the central processing unit. The event manager module is adapted for receiving results of the scanning from the scanning module. The event manager module is further adapted to execute an event based on the results of the scanning. Additionally, the central processing unit is conditionally allowed to read the data saved in the storage and write data to the storage based on the results of the scanning (e.g. item 419 of Figure 4 and item 519 of Figure 5), and a user is

allowed to disable the scanning module. Further, data is precluded from being transmitted between the storage and the central processing unit upon the disabling of the scanning module (e.g. items 404, 418 and 416 of Figure 4). Note page 5, line 13 – page 12, line 23, for example.

With respect to a summary of Claim 39, the above summaries of Claims 1 and 35 are incorporated, at least in part, by reference. As further illustrated in Figure 2, a system is provided for scanning data read from storage, and includes means for saving data therein (e.g. item 202 of Figure 2) and means for controlling access to the data saved therein (e.g. item 206 of Figure 2). In addition, means for issuing read requests are included for reading the data saved therein for processing purposes and write requests for writing data to the storage (e.g. item 204 of Figure 2) along with means for identifying the requests from the central processing unit, and scanning the data for malicious code in response to the requests (e.g. item 208 of Figure 2). Further included are means for receiving results of the scanning from the scanning means and executing an event based on the results of the scanning (e.g. item 206 of Figure 2). Such means (e.g. item 206 of Figure 2) is thus conditionally allowed to read the data saved in the storage and write data to the storage based on the results of the scanning (e.g. item 419 of Figure 4 and item 519 of Figure 5) and a user is allowed to disable the scanning means, and data is precluded from being transmitted between the storage and such means upon the disabling of the scanning means (e.g. items 404, 418 and 416 of Figure 4). Note page 5, line 18 – page 6, line 23, for example.

VI GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL (37 C.F.R. § 41.37(c)(1)(vi))

Following, under each issue listed, is a concise statement setting forth the corresponding ground of rejection.

Issue # 1: The Examiner has rejected Claim 42 under 35 U.S.C. 112, first paragraph, as providing new matter not originally described in the Specification.

Issue # 2: The Examiner has rejected Claims 1-2, 4-7, 10-18, 20-23 and 26-40 under 35 U.S.C. 103(a) as being unpatentable over Makita, U.S. Patent No. 2001/0007120, in view of Flint, U.S. Patent No. 6,735,700.

Issue # 3: The Examiner has rejected Claim 41 under 35 U.S.C. 103(a) as being unpatentable over Makita, U.S. Patent No. 2001/0007120, in view of Flint, U.S. Patent No. 6,735,700, in further view of Browne, U.S. Patent No. 6,272,533.

VII ARGUMENT (37 C.F.R. § 41.37(c)(1)(vii))

The claims of the groups noted below do not stand or fall together. In the present section, appellant explains why the claims of each group are believed to be separately patentable.

Issue #1:

The Examiner has rejected Claim 42 under 35 U.S.C. 112, first paragraph, as providing new matter not originally described in the Specification.

Group #1: Claims 42 and 43

Specifically, the Examiner has stated that '[n]o where in the Specification does the appellant describe that it is determined whether the storage is disabled "only after" determining whether the scanning module is disabled.' Appellant respectfully disagrees with such rejection in view of the clear support for such claim language in Figure 5 of appellant's originally-filed application, as shown below.

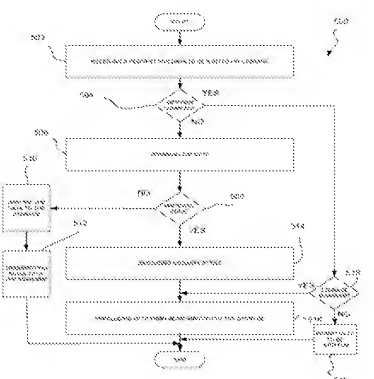

Figure 5

Appellant points out step 504 of Figure 5, wherein it is first determined whether the scanner is disabled. Next, and only if the scanner has been disabled, as depicted by the Yes arrow from 504, is it next determined if the storage is disabled (operation 518). Thus, operation 518 occurs, as shown, only after operation 504 (and not after any other operations shown). To this end, appellant's claimed technique "wherein it is determined whether the storage is disabled only after determining whether the scanning module is disabled" (see Claim 42) is fully supported by the specification with regard to Figure 5.

It is noted that the Examiner has rejected Claim 43 as being dependent on Claim 42. In view of the remarks made hereinabove, a notice of allowance or a specific prior art showing of all of such claim limitations, in combination with the remaining claim elements, is respectfully requested.

Issue #2:

The Examiner has rejected Claims 1-2, 4-7, 10-18, 20-23 and 26-40 under 35 U.S.C. 103(a) as being unpatentable over Makita, U.S. Patent No. 2001/0007120, in view of Flint, U.S. Patent No. 6,735,700.

Group #1: Claims 1, 2, 4, 5, 10, 11, 15-17, 18, 20, 21, 26, 27, 31-34 and 39

With respect to Claim 1, the Examiner continues to rely on the following excerpt from Flint to meet appellant's claimed "wherein a user is allowed to disable the scanning module, and data is precluded from being transmitted from the storage to the central processing unit upon the disabling of the scanning module."

> "The third activity waits for user input (block 421). When user input is received, it is evaluated to determine if the user has requested that a particular file be scanned (block 423). If so, an on-demand scan is performed using the requested file as the scan set as described below with reference to FIG. 6. **If the user input specifies the termination of the anti-virus program (block 427), a termination process illustrated by block 429 and described in more detail below in conjunction with FIG. 8 is performed.** When the user has previously requested the scanning facility be stopped (as described next), the user can request it be restarted (block 431). Any other user input, including a request to stop the scanning facility, is processed at

> block 433. Such user input also includes changing preference parameters that control the overall functioning of the anti-virus software. The user can also specify which files to include in a pre-defined scan set that is used by the on-demand scan of FIG. 6. The handling of such user input is well understood in the art and is not discussed further. Moreover, it will be appreciated that the input interface is conventional and thus not illustrated." (Col. 9, lines 5-24 - emphasis added)

Appellant respectfully asserts that the above excerpt from Flint simply discloses "[i]f the user input specifies the termination of the anti-virus program (block 427), a termination process illustrated by block 429 and described in more detail below in conjunction with FIG. 8 is performed". Thus, Flint only teaches a user terminating the anti-virus program, and not "data is precluded from being transmitted from the storage to the central processing unit upon the disabling of the scanning module," as claimed by appellant.

To further clarify this distinction, appellant respectfully points out Fig. 8 in Flint, as referred to in the above excerpt. Specifically, Fig. 8 teaches writing to permanent storage (block 803) even after a user has specified to terminate the anti-virus program (block 429 of Fig. 4). Appellant respectfully asserts that this clearly *teaches away* from appellant's claim language since appellant specifically claims "data is precluded from being transmitted from the storage to the central processing unit upon the disabling of the scanning module" (emphasis added). Allowing the data to be written to storage or read from storage without fully completing a scan, as in Flint, would provide the opportunity for malicious code to execute and/or proliferate on the systems sought to be protected. Appellant's claimed invention is clearly capable of avoiding such a situation.

In the Advisory Action dated 5/16/2005, the Examiner has argued that Makita, in combination with Flint, teaches appellant's claim language. Specifically, the Examiner has argued that Makita teaches "[t]he storage location retrieves the data and performs an internal virus check on the data before it sends the data back to the cpu (host) ([0180]-[0184])." Additionally, the Examiner has argued that Flint teaches the idea of a user being able to disable and enable a virus scanning module (Col. 9, lines 5-24). From this, the Examiner has concluded that the combination of such teachings meet appellant's claimed method "wherein a user is allowed to disable the scanning module, and data is precluded from being transmitted from the storage to the central processing unit upon the disabling of the scanning module."

Appellant respectfully disagrees. Makita merely teaches two scenarios. First, if a virus is found during the virus check, transmission to the host is stopped ([00183]). Second, if a virus is not found during the virus check, the information is transmitted to the host ([00184]). Clearly, there is no disclosure of the result when no virus check is performed, since Makita does not allow for this option. Thus, only appellant teaches and claims that "data is precluded from being transmitted from the storage to the central processing unit upon the disabling of the scanning module."

To establish a *prima facie* case of obviousness, three basic criteria must be met. First, there must be some suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to modify the reference or to combine reference teachings. Second, there must be a reasonable expectation of success. Finally, the prior art reference (or references when combined) must teach or suggest all the claim limitations. The teaching or suggestion to make the claimed combination and the reasonable expectation of success must both be found in the prior art and not based on appellant's disclosure. *In re Vaeck*, 947 F.2d 488, 20 USPQ2d 1438 (Fed.Cir.1991).

Appellant respectfully asserts that at least the third element of the *prima facie* case of obviousness has not been met, since the prior art references, when combined, fail to teach or suggest all of the claim limitations, as noted above. A notice of allowance or a specific prior art showing of all of appellant's claim limitations, in combination with the remaining claim elements, is respectfully requested.

Group # 2: Claims 35-38

With respect to independent Claim 35, the Examiner has relied on Figure 15 item 413 of Makita to make a prior art showing of appellant's claimed "scanning module coupled to the central processing unit and the storage subsystem controller, the scanning module adapted for identifying the requests from the central processing unit, and scanning the data for malicious code in response to the requests."

Appellant respectfully asserts that item 413 of Figure 15 is a virus check unit to which "information to be recorded corresponding to the command is supplied" (see [0174] in Makita). Having information supplied to a virus check unit simply does not meet "scanning module adapted for identifying requests from the central processing unit," as claimed by appellant (emphasis added).

Further, the Examiner has relied on Makita's disclosed file management unit (Figure 15 item 211) and the following excerpts from Makita to make a prior art showing of appellant's claimed "event manager module coupled to the scanning module and the central processing unit, the event manager module adapted for receiving results of the scanning from the scanning module, the event manager module adapted to execute an event based on the results of the scanning":

> "The file management unit 121 manages the storage of files into, the readout and deletion of files from, and access rights o the recording medium 4 of the external storage 120. The file management unit 121 includes programs for managing the recording medium 4 formatted into a desired logical format in formats corresponding to operation systems such as 12-bit FAT (File Allocation Table) of MS-DOS, the 16-bit FAT of MS-DOS, and UNIX." [0091]
>
> "When a virus is discovered in step S8-5, a transmission to the host computer 110 is stopped, and the host computer 110 is notified that the virus is discovered (step S8-6)." [0183]

Appellant respectfully asserts that a file management unit that manages files, manages access to files, and manages the formatting of files along with stopping a transmission to the host computer when a virus is discovered as disclosed in Makita (see excerpts above) fails to meet "the event manager module adapted for receiving results of the scanning from the scanning module, the event manager module adapted to execute an event based on the results of the scanning," as claimed by appellant (emphasis added). Simply nowhere in Makita is there any suggestion of an "event manager module" that is "adapted for receiving results of the scanning" and "adapted to execute an event based on the results of the scanning," as claimed.

In the Advisory Action dated 5/16/2005, the Examiner has relied on paragraph [0174] of Makita in arguing that the CPU in Makita sends a request to the scanning module to scan for data. Thus, the Examiner has concluded that the scanning module must be adapted for identifying the requests from the CPU since it is adapted to receive requests for a data scan.

Appellant respectfully asserts that Makita merely teaches that "[w]hen a command to record information on the recording medium 4 is supplied from the host computer 110 (step S7-1), information to be recorded corresponding to the command is supplied to the virus check engine unit 413" (emphasis added). Thus, the virus check engine in Makita is not adapted for identifying requests, since no request is ever made by the host computer. In particular, the information in Makita is simply supplied to the virus check engine, and a request is not utilized. To emphasize, the host computer in Makita does not send a request to the scanner, but simply sends the information to the scanner. Thus, the scanner in Makita does not have a request to identify or respond to since it is only the information itself which is being sent to the scanner and not a request.

In addition, in the Advisory Action dated 5/16/2005, the Examiner has relied on the file management unit as described in Makita paragraph [0091], in supporting the present rejection. However, appellant respectfully asserts that such file management unit simply manages "the storage of files into, the readout and deletion of files from, and access rights to the recording medium 4 of the external storage 120" ([0091]). Thus, the file management unit only manages files with respect to the recording medium.

In Makita, the only mention of scanning such files relates to scanning them when information is read out from the recording medium (see paragraph [0181]). Then, after the scanning, it is determined whether the file is transferred to a host computer (see paragraphs [0182]-[0184]). Since the file management unit only manages files with respect to the recording medium, such file management unit does not manage files with respect to their transmission from the virus check unit to the host computer. Therefore, clearly appellant's claimed "event manager module coupled to the scanning module and the central processing unit, the event manager module adapted for receiving results of the scanning from the scanning module, the event manager module adapted to execute an event based on the results of the scanning" has not been met by the Makita reference.

Again, at least the third element of the *prima facie* case of obviousness has not been met, since the prior art references, when combined, fail to teach or suggest all of the claim limitations, as

noted above. A notice of allowance or a specific prior art showing of all of appellant's claim limitations, in combination with the remaining claim elements, is respectfully requested.

Group # 3: Claims 6 and 22

With respect to dependent Claim 6 et al., the Examiner has relied on Makita's paragraph [0213] to meet appellant's claimed technique "wherein the scanning module includes software." Appellant respectfully asserts that paragraph [0213] of Makita simply teaches that the "virus check can be performed even if a virus check program is not installed on the host computer." Thus, the only virus check software program disclosed in Makita relates to a virus checker on the host computer, and not that the scanning module (i.e. virus checker) includes software.

Again, at least the third element of the *prima facie* case of obviousness has not been met, since the prior art references, when combined, fail to teach or suggest all of the claim limitations, as noted above. A notice of allowance or a specific prior art showing of all of appellant's claim limitations, in combination with the remaining claim elements, is respectfully requested.

Group # 4: Claims 7 and 23

With respect to dependent Claim 7 et al., the Examiner has relied on Figure 15 of Makita to meet appellant's claimed technique "wherein the scanning module includes hardware." Appellant respectfully asserts that Figure 15 merely shows that the virus check unit 413 is included in the external storage 4 (which may include logic stored on the external storage 4) and not that the virus check unit includes hardware itself.

Again, at least the third element of the *prima facie* case of obviousness has not been met, since the prior art references, when combined, fail to teach or suggest all of the claim limitations, as noted above. A notice of allowance or a specific prior art showing of all of appellant's claim limitations, in combination with the remaining claim elements, is respectfully requested.

Group # 5: Claims 12, 13 and 28

With respect to dependent Claim 12 et al., the Examiner has relied on paragraph [0183] of Makita to make a prior art showing of appellant's claimed technique "wherein the event includes disabling the scanning module in response to the event." Appellant respectfully asserts that the above cited reference from Makita merely teaches that "a transmission to the host computer 110 is stopped" ([0183]). Thus, there is simply no disclosure of any sort of "disabling [of] the scanning module" and especially not "in response to the event," as claimed by appellant.

Again, at least the third element of the *prima facie* case of obviousness has not been met, since the prior art references, when combined, fail to teach or suggest all of the claim limitations, as noted above. A notice of allowance or a specific prior art showing of all of appellant's claim limitations, in combination with the remaining claim elements, is respectfully requested.

Group # 6: Claims 14 and 30

With respect to dependent Claim 14 et al, the Examiner has relied on Makita's teaching of formatting the recording medium ([0053]-[0054]) to make a prior art showing of appellant's claimed technique "wherein the scanning includes content scanning." The Examiner has stated that content scanning is used to determine a format of the data and to format the data. However, Makita clearly only teaches formatting the recording medium (see specifically paragraph [0054]) and not providing content scanning of the requested data for malicious code, in the manner claimed by appellant.

Again, at least the third element of the *prima facie* case of obviousness has not been met, since the prior art references, when combined, fail to teach or suggest all of the claim limitations, as noted above. A notice of allowance or a specific prior art showing of all of appellant's claim limitations, in combination with the remaining claim elements, is respectfully requested.

Group # 7: Claim 40

With respect to dependent Claim 40, the Examiner has continued to rely on Flint's disclosed system where "[t]he user or administrator also faces the challenges inherent in maintaining the

external database" (Col. 2, lines 19-20) to make a prior art showing of appellant's claimed technique "wherein the user includes a remote administrator."

Appellant respectfully asserts that Flint's basic mention of an administrator that maintains an external database does not meet appellant's "user [that] includes a remote administrator" (Claim 40) in the context of appellant's claim language, such that the "user is allowed to disable the scanning module" (see independent Claim 1).

In the Advisory Action dated 5/16/2005, the Examiner argued that Flint does not provide support for a user being an administrator, but that Flint discloses that a user or administrator can maintain a similar system to that of Makita's and appellant's. The Examiner then concludes by stating that "Flint provides support that a user can be an administrator."

Appellant respectfully asserts that the Examiner's arguments are not clear. First the Examiner states that Flint does not support a user being an administrator, and then the Examiner goes on to state that Flint does provide support that a user can be an administrator. Appellant again argues that the only administrator disclosed in Flint relates to an administrator who maintains a database, and not a remote administrator who can disable the scanning module, as claimed by appellant (see Claim 40 which depends from Claim 1).

Again, at least the third element of the *prima facie* case of obviousness has not been met, since the prior art references, when combined, fail to teach or suggest all of the claim limitations, as noted above. A notice of allowance or a specific prior art showing of all of appellant's claim limitations, in combination with the remaining claim elements, is respectfully requested.

Issue # 3:

The Examiner has rejected Claim 41 under 35 U.S.C. 103(a) as being unpatentable over Makita, U.S. Patent No. 2001/0007120, in view of Flint, U.S. Patent No. 6,735,700, in further view of Browne, U.S. Patent No. 6,272,533.

Group # 1: Claim 41

With respect to dependent Claim 41, the Examiner has relied on Browne to make a prior art showing of appellant's claimed technique "wherein the user is allowed to disable the storage, and the data is precluded from being transmitted to the storage from the central processing unit upon the disabling of the storage." Specifically, the Examiner has stated that Browne discloses a secure computing system in which a manual switch can be pressed so that data is precluded from being written to a storage device.

Appellant respectfully asserts that Browne merely teaches the "disabling [of the] alteration of data residing on a mass storage device" (see Abstract). Thus, simply disabling the alteration of data, as in Browne, does not meet appellant's specifically claimed "disabling of the storage," let alone disabling the storage such that "data is precluded from being transmitted to the storage from the central processing unit upon the disabling of the storage."

Again, appellant respectfully asserts that at least the third element of the *prima facie* case of obviousness has not been met, since the prior art references, when combined, fail to teach or suggest all of the claim limitations, as noted above.

In view of the remarks set forth hereinabove, all of the independent claims are deemed allowable, along with any claims depending therefrom.

VIII CLAIMS APPENDIX (37 C.F.R. § 41.37(c)(1)(viii))

The text of the claims involved in the appeal (along with associated status information) is set forth below:

The text of the claims involved in the appeal (along with associated status information) is set forth below:

1. (Previously Presented) A method for scanning data read from storage, comprising:

a) receiving a request for data saved in storage from a central processing unit;

b) scanning the requested data for malicious code; and

c) transmitting the data from the storage to the central processing unit if malicious code is not found in the data during the scanning;

wherein the scanning is performed by a scanning module coupled to a storage subsystem controller;

wherein a user is allowed to disable the scanning module, and data is precluded from being transmitted from the storage to the central processing unit upon the disabling of the scanning module.

2. (Original) The method as recited in claim 1, wherein the storage is selected from the group consisting of a hard drive, compact disc-read only memory (CD-ROM), and a floppy disk.

3. (Cancelled)

4. (Previously Presented) The method as recited in claim 1, wherein the storage subsystem controller is coupled to a storage driver which is coupled to the central processing unit, where the storage driver is coupled between the storage subsystem controller and the central processing unit, so that the storage subsystem controller and the central processing unit must communicate therethrough.

5. (Previously Presented) The method as recited in claim 1, wherein the storage subsystem controller is coupled to the storage.

6. (Previously Presented) The method as recited in claim 1, wherein the scanning module includes software.

7. (Previously Presented) The method as recited in claim 1, wherein the scanning module includes hardware.

8. (Cancelled)

9. (Cancelled)

10. (Original) The method as recited in claim 1, and further comprising executing an event based on results of the scanning.

11. (Original) The method as recited in claim 10, wherein the event includes an alert.

12. (Original) The method as recited in claim 10, and further comprising disabling the scanning module in response to the event.

13. (Original) The method as recited in claim 12, wherein data is precluded from being transmitted from the storage to the central processing unit upon the disabling of the scanning module.

14. (Original) The method as recited in claim 1, wherein the scanning includes content scanning.

15. (Original) The method as recited in claim 1, wherein the scanning includes virus scanning.

16. (Original) The method as recited in claim 1, wherein the storage is accessible via a network.

17. (Previously Presented) A computer program product for scanning data read from storage, comprising:

a) computer code for receiving a request for data saved in storage from a central processing unit;

b) computer code for scanning the requested data for malicious code; and

c) computer code for transmitting the data from the storage to the central processing unit if malicious code is not found in the data during the scanning;

wherein the scanning is performed by a scanning module coupled to a storage subsystem controller;

wherein a user is allowed to disable the scanning module, and data is precluded from being transmitted from the storage to the central processing unit upon the disabling of the scanning module.

18. (Original) The computer program product as recited in claim 17, wherein the storage is selected from the group consisting of a hard drive, compact disc-read only memory (CD-ROM), and a floppy disk.

19. (Cancelled)

20. (Previously Presented) The computer program product as recited in claim 17, wherein the storage subsystem controller is coupled to a storage driver which is coupled to the central processing unit, where the storage driver is coupled between the storage subsystem controller and the central processing unit, so that the storage subsystem controller and the central processing unit must communicate therethrough.

21. (Previously Presented) The computer program product as recited in claim 17, wherein the storage subsystem controller is coupled to the storage.

22. (Previously Presented) The computer program product as recited in claim 17, wherein the scanning module includes software.

23. (Previously Presented) The computer program product as recited in claim 17, wherein the scanning module includes hardware.

24. (Cancelled)

25. (Cancelled)

26. (Original) The computer program product as recited in claim 19, and further comprising computer code for executing an event based on results of the scanning.

27. (Original) The computer program product as recited in claim 26, wherein the event includes an alert.

28. (Original) The computer program product as recited in claim 26, and further comprising computer code for disabling the scanning module in response to the event.

29. (Original) The computer program product as recited in claim 28, wherein data is precluded from being transmitted from the storage to the central processing unit upon the disabling of the scanning module.

30. (Original) The computer program product as recited in claim 17, wherein the scanning includes content scanning.

31. (Original) The computer program product as recited in claim 17, wherein the scanning includes virus scanning.

32. (Original) The computer program product as recited in claim 17, wherein the storage is accessible via a network.

33. (Previously Presented) A method for scanning data written to storage, comprising:

a) receiving a request for data to be written in storage, the request being received from a central processing unit;

b) scanning the data for malicious code; and

c) writing the data to the storage if malicious code is not found in the data during the scanning;

wherein the scanning is performed by a scanning module coupled to a storage subsystem controller;

wherein a user is allowed to disable the scanning module, and data is precluded from being transmitted to the storage from the central processing unit upon the disabling of the scanning module.

34. (Previously Presented) A computer program product for scanning data written to storage, comprising:

a) computer code for receiving a request for data to be written in storage, the request being received from a central processing unit;

b) computer code for scanning the data for malicious code; and

c) computer code for writing the data to the storage if malicious code is not found in the data during the scanning;

wherein the scanning is performed by a scanning module coupled to a storage subsystem controller;

wherein a user is allowed to disable the scanning module, and data is precluded from being transmitted to the storage from the central processing unit upon the disabling of the scanning module.

35. (Previously Presented) A system for scanning data read from storage, comprising:

a) storage for saving data therein;

b) a storage subsystem controller coupled to the storage for controlling access to the data saved therein;

c) a central processing unit coupled to the storage subsystem controller for issuing read requests for reading the data saved therein for processing purposes, and write requests for writing data to the storage;

d) a scanning module coupled to the central processing unit and the storage subsystem controller, the scanning module adapted for identifying the requests from the central processing unit, and scanning the data for malicious code in response to the requests; and

e) an event manager module coupled to the scanning module and the central processing unit, the event manager module adapted for receiving results of the scanning from the scanning module, the event manager module adapted to execute an event based on the results of the scanning;

f) wherein the central processing unit is conditionally allowed to read the data saved in the storage and write data to the storage based on the results of the scanning;

g) wherein a user is allowed to disable the scanning module, and data is precluded from being transmitted between the storage and the central processing unit upon the disabling of the scanning module.

36. (Original) The system as recited in claim 35, wherein the scanning module is coupled to the storage subsystem controller via a bus.

37. (Original) The system as recited in claim 35, wherein the scanning module is directly coupled to the storage subsystem controller.

38. (Previously Presented) The system as recited in claim 35, wherein the scanning module is coupled to the storage subsystem controller via a storage driver, where the storage driver is coupled between the storage subsystem controller and the central processing unit, so that the storage subsystem controller and the central processing unit must communicate therethrough.

39. (Previously Presented) A system for scanning data read from storage, comprising:

a) means for saving data therein;

b) means for controlling access to the data saved therein;

c) means for issuing read requests for reading the data saved therein for processing purposes and write requests for writing data to the storage;

d) means for identifying the requests from the central processing unit, and scanning the data for malicious code in response to the requests; and

e) means for receiving results of the scanning from the scanning module, the event manager module adapted to execute an event based on the results of the scanning;

f) wherein the central processing units is conditionally allowed to read the data saved in the storage and write data to the storage based on the results of the scanning;

g) wherein a user is allowed to disable the scanning module, and data is precluded from being transmitted between the storage and the central processing unit upon the disabling of the scanning module.

40. (Previously Presented) The method as recited in claim 1, wherein the user includes a remote administrator.

41. (Previously Presented) The method as recited in claim 1, wherein the user is allowed to disable the storage, and the data is precluded from being transmitted to the storage from the central processing unit upon the disabling of the storage.

42. (Previously Presented) The method as recited in claim 41, wherein it is determined whether the storage is disabled only after determining whether the scanning module is disabled.

43. (Previously Presented) The method as recited in claim 42, wherein the disabling and enabling of the storage and the scanning module provides increased functionality in conditionally precluding transmission of the data to the storage from the central processing unit.

IX EVIDENCE APPENDIX (37 C.F.R. § 41.37(c)(1)(ix))

There is no such evidence.

X RELATED PROCEEDING APPENDIX (37 C.F.R. § 41.37(c)(1)(x))

There is no such related proceeding.

In the event a telephone conversation would expedite the prosecution of this application, the Examiner may reach the undersigned at (408) 971-2573. For payment of any additional fees due in connection with the filing of this paper, the Commissioner is authorized to charge such fees to Deposit Account No. 50-1351 (Order No. NAI1P020).

Respectfully submitted,

By: /KEVINZILKA/ Date: October 22, 2007
Kevin J. Zilka
Reg. No. 41,429

Zilka-Kotab, P.C.
P.O. Box 721120
San Jose, California 95172-1120
Telephone: (408) 971-2573
Facsimile: (408) 971-4660

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/916,600	07/26/2001	Chris A. Barton	NAI1P020/01.139.01	8707

28875 7590 09/21/2007

Zilka-Kotab, PC
P.O. BOX 721120
SAN JOSE, CA 95172-1120

EXAMINER	
PYZOCHA, MICHAEL J	

ART UNIT	PAPER NUMBER
2137	

MAIL DATE	DELIVERY MODE
09/21/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notification of Non-Compliant Appeal Brief (37 CFR 41.37)	Application No. 09/916,600	Applicant(s) BARTON ET AL.	
	Examiner Michael Pyzocha	Art Unit 2137	

--The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

The Appeal Brief filed on 05 October 2006 is defective for failure to comply with one or more provisions of 37 CFR 41.37.

To avoid dismissal of the appeal, applicant must file anamended brief or other appropriate correction (see MPEP 1205.03) within **ONE MONTH or THIRTY DAYS** from the mailing date of this Notification, whichever is longer. **EXTENSIONS OF THIS TIME PERIOD MAY BE GRANTED UNDER 37 CFR 1.136.**

1. ☐ The brief does not contain the items required under 37 CFR 41.37(c), or the items are not under the proper heading or in the proper order.

2. ☒ The brief does not contain a statement of the status of all claims, (e.g., rejected, allowed, withdrawn, objected to, canceled), or does not identify the appealed claims (37 CFR 41.37(c)(1)(iii)).

3. ☒ At least one amendment has been filed subsequent to the final rejection, and the brief does not contain a statement of the status of each such amendment (37 CFR 41.37(c)(1)(iv)).

4. ☐ (a) The brief does not contain a concise explanation of the subject matter defined in each of the independent claims involved in the appeal, referring to the specification by page and line number and to the drawings, if any, by reference characters; and/or (b) the brief fails to: (1) identify, for each independent claim involved in the appeal and for each dependent claim argued separately, every means plus function and step plus function under 35 U.S.C. 112, sixth paragraph, and/or (2) set forth the structure, material, or acts described in the specification as corresponding to each claimed function with reference to the specification by page and line number, and to the drawings, if any, by reference characters (37 CFR 41.37(c)(1)(v)).

5. ☒ The brief does not contain a concise statement of each ground of rejection presented for review (37 CFR 41.37(c)(1)(vi))

6. ☒ The brief does not present an argument under a separate heading for each ground of rejection on appeal (37 CFR 41.37(c)(1)(vii)).

7. ☒ The brief does not contain a correct copy of the appealed claims as an appendix thereto (37 CFR 41.37(c)(1)(viii)).

8. ☐ The brief does not contain copies of the evidence submitted under 37 CFR 1.130, 1.131, or 1.132 or of any other evidence entered by the examiner **and relied upon by appellant in the appeal**, along with a statement setting forth where in the record that evidence was entered by the examiner, as an appendix thereto (37 CFR 41.37(c)(1)(ix)).

9. ☐ The brief does not contain copies of the decisions rendered by a court or the Board in the proceeding identified in the Related Appeals and Interferences section of the brief as an appendix thereto (37 CFR 41.37(c)(1)(x)).

10. ☒ Other (including any explanation in support of the above items):

See Continuation Sheet.

EMMANUEL L. MOISE
SUPERVISORY PATENT EXAMINER

Continuation of 10. Other (including any explanation in support of the above items): Amendment filed April 28, 2005 included the cancellation of claim 13, the Amendment after final was denied entry by the Examiner in an Adivosry Action dated May 15, 2005.

The Status of Claims section identifies claim 13 as cancelled but it is pending and under rejection

In the Grounds of rejection to be reviewed on appeal section, Issue #2 lists claims 1-40 as rejected under 35 USC 103(a), however, claims 3, 8, 9, 19, 24, and 25 were cancelled in the Amendment dated January 28, 2005.

The argument section appellant incorporates original claim 3 into part d above and original claims 8 and 9; all identified claims which have been cancelled.

The Claims Appendix lists claim 13 as cancelled, however as noted above it remains pending.